February 14, 2018

Chairman Greg Walden
United States House of Representatives
Committee on Energy and Commerce
Washington, D.C. 20515

Chairman Marsha Blackburn
United States House of Representatives
Subcommittee on Communications and Technology
Washington, D.C. 20515

Chairman Robert E. Latta
United States House of Representatives
Subcommittee on Digital Commerce and Consumer Protection
Washington, D.C. 20515

Chairman Gregg Harper
United States House of Representatives
Subcommittee on Oversight and Investigations
Washington, D.C. 20515

Dear Chairman Walden, Chairman Blackburn, Chairman Latta, and Chairman Harper,

Thank you for your letter concerning recently uncovered security risks known as "Meltdown" and "Spectre." Apple is deeply committed to protecting the privacy and security of our customers, and we devote significant time and energy to keeping our products secure.

It is important to note that these vulnerabilities were identified as part of a research effort, and we are aware of no affected users. Regardless, we have released several mitigations for Meltdown and Spectre, and we continue to monitor and assess the risks posed by these threats.

Meltdown and Spectre apply to most modern processors and affect nearly all computing devices and operating systems. They take advantage of a modern computer processing unit (CPU) performance feature called speculative execution. Meltdown and Spectre abuse this performance feature to allow unauthorized access to privileged memory. Of our products, Meltdown and Spectre potentially affected devices that run iOS, macOS, and tvOS, but not Apple Watch.

Apple often works with companies across the industry to protect its products, networks, and users from a variety of risks, including through standard

coordinated vulnerability disclosure practices. When threats like Meltdown and Spectre are discovered, companies work first to develop fixes to these threats and implement mitigations before notifying users, in order to minimize the opportunity for bad actors to exploit the flaws.

In June 2017, Apple learned from ARM about three vulnerabilities impacting their chipsets that are referred to as Spectre and Meltdown. In July 2017, Intel similarly notified Apple that these vulnerabilities impacted chips they produce that are used in Mac computers. We understand that ARM and Intel learned of these vulnerabilities from Google (Project Zero).

As is standard industry practice, Apple (like other notified vendors) was required to agree not to disclose the vulnerabilities for ninety days. Requiring companies not to disclose the vulnerabilities for a set time allows the companies to do the technical work needed to verify, test, and remediate the vulnerability while protecting the public from harm. Ninety days is a standard initial period for such an embargo.

The ninety-day period can be extended for a variety of reasons, including where, as in this case, there was no known exploitation of the vulnerability and mitigations require deep and architectural changes in the software and hardware layers that cannot be completed in ninety days. Multiple stakeholders supported extending the ninety-day period to early January to allow additional time to remediate the vulnerabilities. Google (Project Zero), as the "finder" of the vulnerabilities, agreed the extension was in the public interest.

Apple released fixes for Meltdown and Spectre as quickly as possible. Beginning in December, we issued a series of updates containing mitigations in iOS 11.2, macOS 10.13.2, and tvOS 11.2 (to help defend against Meltdown); and in iOS 11.2.2, the macOS High Sierra 10.13.2 Supplemental Update, and Safari 11.0.2 for macOS Sierra and OS X El Capitan (to help defend against Spectre).

Once the embargo was lifted, we were able to publicly disclose details about the issue and mitigations.

Please find answers to your specific questions below.

1. Why was an information embargo related to the Meltdown and Spectre vulnerabilities imposed?

It is a standard best practice to embargo the disclosure of vulnerabilities so that affected entities can take steps to protect their systems and customers. This minimizes the time that such information can be exploited by bad actors and

allows companies to implement mitigations as expeditiously as possible. When multiple parties are involved, they coordinate vulnerability disclosure to limit the risk to end users. Vulnerability disclosure best practices continue to develop and evolve, but representative frameworks include the NTIA Guidelines and Practices for Multiple Vulnerability Coordination and Disclosure.

2. What company or combination of companies proposed the embargo?

Apple had no role in proposing or establishing the initial ninety-day period. Apple was among the stakeholders supporting an extension of the period to January 2018 to allow for adequate testing and release of fixes. We believe this extension was necessary to facilitate the complicated technical changes necessary to mitigate the risk to consumers.

3. When was the United States Computer Emergency Readiness Team (US-CERT) informed of the vulnerabilities?

The United States Computer Emergency Readiness Team usually engages with the vendor that assigns the Common Vulnerabilities and Exposures (CVE) number, which in this case was not Apple. We do not know when the United States Computer Emergency Readiness Team was informed of Meltdown or Spectre.

4. When was the Computer Emergency Readiness Team Coordination Center (CERT/CC) informed of the vulnerabilities?

The Computer Emergency Readiness Team Coordination Center usually engages with the vendor that assigns the CVE number, which was not Apple in this case. We do not know when the United States Computer Emergency Readiness Team Coordination Center was informed of Meltdown or Spectre.

5. Did your company perform any analyses to determine whether the embargo could have any negative impacts on critical infrastructure sectors such as healthcare and energy that rely on affected products?

Our urgent focus after learning about Spectre and Meltdown was on verifying the findings and on developing, testing, and ultimately releasing fixes for the affected Apple products. Because we make the same products for personal, business, or government use, the mitigations help safeguard all of our users, including those in energy and healthcare. The embargo was consistent with industry best practice, which allows an opportunity to mitigate risks to users before publication of the flaw to limit the ability of bad actors to take advantage before mitigation is in place.

6. Did your company perform any analyses to determine whether the embargo could have any negative impacts on other information technology companies that rely on affected products?

Apple did not design the CPU architectures where the vulnerabilities reside, nor were we the "finder" of the vulnerabilities. As such, Apple did not assess the embargo's broader impacts, rather our focus was on evaluating the risks to our systems and users. We developed and expeditiously made available mitigations for iOS, macOS, tvOS, and Safari. Once the embargo was lifted, we publicly disclosed details of the mitigations.

7. What resources or best practices did your company use in deciding to implement the embargo?

Public release prior to remediation increases risk to affected users. The initial stakeholders (Google (Project Zero) as the "finder" and ARM and Intel) determined the disclosure scope and timeline for the initial embargo. Trusted communication channels were established, so that the downstream vendors like Apple could receive the necessary technical details to allow for assessment, validation, and remediation of the vulnerabilities. We worked hard to develop fixes, and, in line with best practices where a security vulnerability is not known or exploited outside the circle of trusted stakeholders, we advocated for additional time when it became apparent that more work would be required prior to remediation.

9. Based on your company's experience during this process, has your company established lessons learned relating to multi-party coordinated vulnerability disclosure?

As a downstream party that uses CPUs impacted by these vulnerabilities, we continue to study, test, and refine our technical response to variants of the Meltdown and Spectre vulnerabilities. To date, there are still no known users affected by these vulnerabilities. We always welcome dialogue about ways to augment best practices around coordinated vulnerability disclosure.

We appreciate your attention to this issue and the opportunity to address your questions.

Sincerely,

Cynthia C. Hogan
Vice President for Public Policy, Americas
Apple